ZARZADZENIE NR 164/2017
BURMISTRZA GŁOWNA
z dnia 27 listopada 2017 r.

w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Miejskim w Głownie oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Głownie.

Na podstawie art. 33 ust. 2 i 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2017 r. poz. 1875, poz. 2232) oraz art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 poz. 922) w związku § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024)

zarządzam, co następuje:

§ 1. Wprowadzam Politykę bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Miejskim w Głownie, stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§ 2. Wprowadzam Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Głownie, stanowiącą załącznik nr 2 do niniejszego zarządzenia.

§ 3. Traci moc Zarządzenie nr 18/2015 Burmistrza Głowna z dnia 2 marca 2015 r. w sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Miejskim w Głownie oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Głownie, zmienione zarządzeniem nr 86/2015 Burmistrza Głowna z dnia 26 czerwca 2015 r., zarządzeniem nr 129/2016 Burmistrza Głowna z dnia 30 sierpnia 2016 r., zarządzeniem nr 104/2017 Burmistrza Głowna z dnia 3 sierpnia 2017 r.

§ 4. Wykonanie Zarządzenia powierzam Sekretarzowi Miasta Głowna.

§ 5. Zarządzenie wchodzi w życie z dniem podjęcia i podlega ogłoszeniu zgodnie z obowiązującymi przepisami.

Burmistrz Głowna
/-/
Grzegorz Janeczek

Załącznik Nr 1
do Zarządzenia Nr 164/2017
Burmistrza Głowna
z dnia 27 listopada 2017 r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH PRZETWARZANYCH W URZĘDZIE MIEJSKIM W GŁOWNIE

SPIS TREŚCI

ROZDZIAŁ 1 WYKAZ SKRÓTÓW I DEFINICJI

SKRÓTY	
UODO	Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
Rozporządzenie MSWiA	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie sposobu przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
Urząd	Urząd Miejski w Głownie ul. Młynarska 15, 95-015 Głowno (wraz z innymi lokalizacjami).
ADO	Administrator Danych Osobowych w Urzędzie Miejskim w Głownie.
ASI/ Informatyk Urzędu	Administrator Systemu/ Administrator Systemu Informatycznego – Starszy Informatyk w Urzędzie Miejskim w Głownie.
Polityka bezpieczeństwa	Polityka bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Miejskim w Głownie.
Instrukcja	Instrukcja zarządzania systemem informatycznym w Urzędzie Miejskim w Głownie.
GIODO	Generalny Inspektor Ochrony Danych Osobowych

DEFINICJE	
Administrator Danych Osobowych	Podmiot decydujący o celach i środkach przetwarzania danych osobowych w Urzędzie – Burmistrz Głowna.
Administrator Systemów Informatycznych	Pracownik Urzędu wyznaczony przez Burmistrza (ADO), odpowiedzialny za funkcjonowanie infrastruktury informatycznej oraz za stosowanie technicznych środków bezpieczeństwa w tych systemach – **Informatyk Urzędu.**
Dane osobowe	Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
Zbiór danych osobowych	Każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów
Użytkownik	Osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym Urzędu i posiadająca w nim aktywny profil użytkownika zabezpieczony hasłem dostępu. Użytkownikiem może być pracownik Urzędu, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż lub praktyki w Urzędzie, jeżeli posiada stosowne upoważnienie do przetwarzania danych osobowych.
Osoba uprawniona/ upoważniona	Każda osoba posiadająca ważne upoważnienie do przetwarzania danych osobowych nadane przez ADO.
System informatyczny	Zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
Wykaz zbiorów danych osobowych	Wykaz zarejestrowanych oraz nie podlegających rejestracji zbiorów danych osobowych przetwarzanych w Urzędzie.
Przetwarzanie danych	Jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
Sieć lokalna	Połączenie systemów informatycznych Urzędu wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.

Sieć publiczna	Sieć publiczna w rozumieniu ustawy z dnia16 lipca 2004r. - Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907 z późn. zm.)
Identyfikator Użytkownika	Ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
Użytkownik zewnętrzny	Osoba nie będącą pracownikiem, wolontariuszem lub stażystą Urzędu Miejskiego w Głownie, posiadająca uprawnienia do przetwarzania informacji w związku z wykonywaniem czynności na rzecz Urzędu.
Zabezpieczenie danych osobowych	Środki administracyjne, techniczne i fizyczne wdrożone w celu zabezpieczenia zasobów technicznych oraz ochrony przed zniszczeniem, nieuprawnionym dostępem i modyfikacją, ujawnieniem lub pozyskaniem danych osobowych bądź ich utratą.
Integralność danych	Właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
Poufność danych	Właściwość zapewniająca, że dane osobowe nie są udostępniane nieupoważnionym osobom.
Dostępność	Właściwość zapewniająca, że dane osobowe są dostępne dla wszystkich upoważnionych osób.
Właściciel danych osobowych	Osoba kierująca komórką organizacyjną, odpowiedzialna za ochronę danych osobowych przetwarzanych w podległej jej komórce.

ROZDZIAŁ 2 CEL DOKUMENTU

Celem polityki bezpieczeństwa jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby zapewnić właściwą ochronę danych osobowych przetwarzanych w Urzędzie Miejskim w Głownie, a w szczególności zabezpieczyć dane przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz ich zmianą, utratą, uszkodzeniem lub zniszczeniem.

„Polityka bezpieczeństwa" określa tryb postępowania w przypadku, gdy:

a) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
b) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.

„Polityka bezpieczeństwa" ma zastosowanie do wszystkich pracowników Urzędu.

Realizacja wymagań tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia akceptowalnego poziomu zabezpieczenia danych osobowych przetwarzanych w systemach informatycznym Urzędu.

Administratorem Danych Osobowych przetwarzanych w Urzędzie jest Burmistrz Głowna.

ROZDZIAŁ 3 ODPOWIEDZIALNOŚĆ

Dokument jest dedykowany wszystkim osobom i podmiotom odpowiedzialnym za prawidłowe funkcjonowanie systemu przetwarzania danych osobowych w Urzędzie oraz za jego eksploatację.

Administrator Danych Osobowych jest zobowiązany do:

a) czuwania nad tym by przetwarzane w Urzędzie dane osobowe były przetwarzane zgodnie z prawem,
b) zapewnienia niezbędnych środków technicznych i organizacyjnych w celu zapewnienia ochrony przetwarzanych w Urzędzie danych osobowych,

c) podziału zadań i obowiązków związanych z organizacją ochrony danych osobowych,
d) zapewnienia dostępności szkoleń dla pracowników w zakresie przepisów o ochronie danych osobowych oraz zagrożeń związanych z ich przetwarzaniem,
e) zapewnienia środków finansowych na merytoryczne przygotowanie osób odpowiedzialnych za nadzór nad ochroną danych osobowych,
f) przyjmowania i zatwierdzania niezbędnych, wymaganych przez przepisy prawa dokumentów regulujących ochronę danych osobowych w Urzędzie,
g) nadawania, zmiany oraz cofania uprawnień do przetwarzania danych osobowych na wniosek:
   - Kierowników referatów,
   - osób sprawujących nadzór nad komórką organizacyjną,

   dla pracowników, wolontariuszy lub stażystów Urzędu oraz użytkowników zewnętrznych (Załącznik nr 4 do Polityki bezpieczeństwa),
h) prowadzenia ewidencji osób upoważnionych przy przetwarzaniu danych osobowych - rejestr osób upoważnionych (Załącznik nr 2 do Polityki bezpieczeństwa),
i) rejestracji w GIODO zbiorów danych osobowych przed przystąpieniem do ich przetwarzania,
j) usuwania niezgodności przepisów wewnętrznych Urzędu z przepisami ustawowymi w zakresie ochrony danych osobowych i przedstawienia stosownych projektów zmian w celu dostosowania ich do regulacji ustawowych,
k) prowadzenia oraz aktualizacji dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych (Zał. Nr 1 – wykaz zbiorów danych osobowych przetwarzanych w Urzędzie Miejskim w Głownie, Zał. Nr 2 – ewidencja osób upoważnionych do przetwarzania danych w Urzędzie),
l) wprowadzania w życie i nadzoru nad przestrzeganiem Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Głownie,
m) nadzorowania i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych,
n) podjęcie natychmiastowych działań na rzecz ochrony danych w przypadku naruszenia UODO.

Administrator Systemu/Administrator Systemu Informatycznego – Informatyk Urzędu realizuje zadania w zakresie zapewnienia ochrony danych osobowych zgodnie z wymaganiami UODO i Rozporządzenia MSWiA, a w szczególności:

a) zapewnia należyty stan techniczny urządzeń służących przetwarzaniu danych osobowych w Urzędzie,
b) zapewnia właściwe funkcjonowanie Aplikacji służących do przetwarzania danych osobowych w Urzędzie,
c) zapewnia właściwy poziom zabezpieczeń danych osobowych przetwarzanych w Urzędzie,
d) nadaje uprawnienia w systemie informatycznym Urzędu,
e) nadzoruje działania mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
f) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,
g) wyrejestrowuje użytkowników na polecenie ADO,
h) sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
i) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów i innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci lokalnej i bezpiecznej teletransmisji,
j) wykonuje i zarządza kopiami bezpieczeństwa oprogramowania systemowego (w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie),

k) współpracuje z ADO przy zapewnieniu odpowiedniego poziomu świadomości pracowników Urzędu w zakresie bezpieczeństwa danych osobowych,

l) współpracuje z ADO w przypadkach naruszenia bezpieczeństwa danych osobowych przetwarzanych w Urzędzie.

Kierownicy komórek organizacyjnych/ osoby sprawujące nadzór nad komórkami organizacyjnymi Urzędu są zobowiązani do:

a) przestrzegania Instrukcji i Polityki bezpieczeństwa,

b) opracowania dla każdej osoby zatrudnionej przy przetwarzaniu danych osobowych zakresu czynności z uwzględnieniem stopnia dostępu do danych osobowych oraz przewidzianej odpowiedzialności za naruszenie tajemnicy danych osobowych,

c) sprawowania nadzoru nad pracą podległych pracowników w zakresie wykonywania czynności służbowych w sposób zapewniający ochronę danych osobowych (poprawności przetwarzania danych osobowych ze względu na ich cel, zakres i czas przetwarzania),

d) zwracania się do ADO o rozstrzygniecie w przypadku istotnych wątpliwości co do stosowania przepisów prawnych z zakresu danych osobowych,

e) niezwłocznego zawiadomienia ADO o konieczności opisania nowego zbioru danych osobowych,

f) wnioskowanie o upoważnienia/ zmianę upoważnień dla podległych sobie pracowników/ stażystów/ wolontariuszy (Załącznik nr 3 do Polityki bezpieczeństwa). Wnioski należy składać w Referacie Organizacyjno–Administracyjnym.

Pracownik/ wolontariusz/ stażysta (niezależnie od formy współpracy) upoważniony do przetwarzania danych osobowych zobowiązany jest do:

a) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych – Oświadczenie o zapoznaniu się z przepisami ustawy, dokumentacji oraz zachowania poufności przetwarzania danych osobowych w Urzędzie (Załącznik Nr 5 do Polityki Bezpieczeństwa),

b) podporządkowania się poleceniom ADO, ASI oraz właściwego kierownika w zakresie ochrony danych osobowych,

c) zachowania w tajemnicy informacji dotyczących przetwarzania danych osobowych w Urzędzie (Załączniki Nr 4 i 5 do Polityki Bezpieczeństwa).

d) stosowania określonych przez ADO środków technicznych i organizacyjnych mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, utratą bądź zniszczeniem,

e) zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych osobowych w celu ochrony interesów osób, których te dane dotyczą.

ROZDZIAŁ 4 ZAKRES DOKUMENTU

Niniejszy dokument opisuje zasady mające zapewnić bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych w Urzędzie, w tym zasobów technicznych i organizacyjnych. Opisane zasady określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających funkcjonowanie Urzędu. Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz określa jakie procedury postępowania opracowano dla zapobiegania i minimalizowania skutków potencjalnych zagrożeń.

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych osobowych oraz ciągłość funkcjonowania systemu informatycznego Urzędu są priorytetowymi celami Urzędu, co mają zapewnić dokumenty opracowane w zakresie ochrony danych osobowych i inne procedury i instrukcje, związane z zapewnieniem wysokiego poziomu bezpieczeństwa systemu informatycznego.

Wszelkie zmiany w konfiguracji środowiska techniczno-systemowego lub w obszarach organizacyjno-prawnych wpływające na zmianę w podejściu do eksploatowanych środków ochrony systemu lub zmieniające bezpośrednio zastosowane środki ochrony muszą być uwzględnione w kolejnych wersjach niniejszego dokumentu.

Politykę Bezpieczeństwa stosuje się do danych osobowych:

- przetwarzanych w systemach informatycznych,
- zapisanych na zewnętrznych nośnikach informacji,
- przetwarzanych tradycyjnie w systemach papierowych.

4.1 AKTY NORMATYWNE

Dokument spełnia następujące wymagania przepisów prawa:

a) Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922).

b) Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 r. Nr 100, poz. 1024)

4.2 REGULACJE WEWNĘTRZNE

-niniejsze Zarządzenie

ROZDZIAŁ 5 POZIOM BEZPIECZEŃSTWA TELEINFORMATYCZNEGO.

W Urzędzie z uwagi na fakt, że urządzenia systemu informatycznego służącego do przetwarzania danych osobowych połączone są z siecią publiczną, stosuje się wysoki poziom bezpieczeństwa teleinformatycznego.

ROZDZIAŁ 6 ZASADY DOPUSZCZANIA PRACOWNIKÓW URZĘDU DO PRZETWARZANIA DANYCH OSOBOWYCH, OBOWIĄZKI NAŁOŻONE NA PRACOWNIKÓW DOPUSZCZONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH ORAZ REJESTRACJA/ AKTUALIZACJA ZBIORU DANYCH DO GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH

6.1 DOPUSZCZENIE PRACOWNIKÓW URZĘDU DO PRZETWARZANIA DANYCH OSOBOWYCH.

a) Do przetwarzania danych osobowych, mogą być dopuszczone wyłącznie osoby posiadające imienne upoważnienie ADO.

b) Kierownik Referatu/ osoba sprawująca nadzór nad komórką organizacyjną po zidentyfikowaniu potrzeby przetwarzania danych osobowych przez podległego pracownika, występuje niezwłocznie z wnioskiem do ADO o wystawienie upoważnienia do przetwarzania danych osobowych (wzór wniosku określa załącznik nr 3 do „Polityki Bezpieczeństwa"). Wniosek może zostać przekazany w formie pisemnej lub elektronicznej. Za poprawność wniosku odpowiedzialna jest osoba składająca.

c) ADO, po stwierdzeniu zasadności otrzymanego wniosku, zleca pracownikowi Referatu Organizacyjno – Administracyjnego opracowanie projektu upoważnienia do przetwarzania danych osobowych oraz przeprowadzenie wstępnego szkolenia z zakresu ochrony danych osobowych.

d) ADO prowadzi Rejestr wydanych upoważnień do przetwarzania danych osobowych (Rejestr Osób Upoważnionych do przetwarzania danych osobowych – wzór rejestru określa załącznik nr 2 do Polityki bezpieczeństwa).

e) Opracowane upoważnienie pracownik Referatu Organizacyjno – Administracyjnego przedkłada do podpisu ADO lub osobie przez niego upoważnionej.

f) W przypadku zmiany zakresu czynności pracownika/ wolontariusza/ stażysty, do których został upoważniony na mocy wydanego upoważnienia, jego bezpośredni przełożony ma obowiązek poinformować o tym ADO.

g) Pracownik potwierdza odbiór upoważnienia, składając na nim podpis.

6.2 OSOBY DOPUSZCZONE DO PRZETWARZANIA DANYCH OSOBOWYCH SĄ ZOBOWIĄZANE DO:

a) Bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania danych osobowych określonych w Polityce Bezpieczeństwa, Instrukcji i innych procedurach obowiązujących w Urzędzie.

b) Przetwarzania danych osobowych tylko w wyznaczonych do tego celu pomieszczeniach służbowych (lub wyznaczonych ich częściach).

c) Zabezpieczania zbiorów danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych za pomocą środków określonych w Polityce Bezpieczeństwa, Instrukcji oraz innych procedurach obowiązujących w Urzędzie.

d) Niszczenia wszystkich zbędnych nośników zawierających dane osobowe w sposób uniemożliwiający ich odczytanie.

e) Nieudzielania informacji o danych osobowych innym podmiotom, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w takich przepisach zostały spełnione.

f) Bezzwłocznego zawiadamiania ADO o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających dane osobowe.

6.3 ZGŁOSZENIE DO REJESTRACJI LUB AKTUALIZACJI ZBIORU DANYCH DO GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH

a) ADO zobowiązany jest zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 UODO.

b) ADO jest obowiązany zgłaszać Generalnemu Inspektorowi Ochrony Danych Osobowych każdą zmianę informacji w zgłoszonym zbiorze w terminie 30 dni od dnia dokonania zmiany w zbiorze danych.

c) Każdy kto zidentyfikował zbiór danych osobowych lub zmiany powstałe w zbiorze danych osobowych przekazuje taką informację ADO.

d) Pracownik Referatu Organizacyjno – Administracyjnego przygotowuje wniosek o zarejestrowanie zbioru danych i przedkłada go do podpisania ADO lub osobie przez niego upoważnionej.

6.4 ZASADY WSTĘPU DO POMIESZCZEŃ, W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

a) Osobami mającymi prawo pobierać klucze do pomieszczeń, w których przetwarzane są dane osobowe są pracownicy danej komórki organizacyjnej.

b) Osobami nie mającym nadanych upoważnień do przetwarzania danych osobowych w Urzędzie, a mającymi wstęp do pomieszczeń, w których przetwarzane są dane osobowe są osoby sprzątające.

c) W pomieszczeniach, w których przetwarzane są dane osobowe od poniedziałku do piątku w godzinach od 8^{00} - 16^{00} przebywają pracownicy/ wolontariusze/ stażyści zatrudnieni przy przetwarzaniu danych osobowych. W uzasadnionych przypadkach po otrzymaniu pisemnej zgody Sekretarza Miasta Głowna, wyznaczeni pracownicy Urzędu mogą przebywać po poza godzinami pracy oraz w dni wolne od pracy na terenie Urzędu.

d) W godzinach od 5^{00} - 14^{00} na terenie Urzędu mogą przebywać osoby sprzątające pomieszczenia biurowe.

ROZDZIAŁ 7 OPIS SYSTEMU

7.1 WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Pomieszczeniami tworzącymi obszar, w którym znajdują się przetwarzane dane osobowe są pomieszczenia w, których znajdują się zbiory danych w formie kartotek, rejestrów i innych oraz stacjonarny sprzęt komputerowy, w którym są przetwarzane dane osobowej:

a) Urząd Miejski w Głownie ul. Młynarska 15; 95-015 Głowno

b) Urząd Miejski w Głownie ul. Dworska 4; 95-015 Głowno

c) Urząd Miejski w Głownie ul. Ludwika Norblina 1; 95-015 Głowno

Szczegółowe informacje dotyczące wykazu pomieszczeń w których przetwarzane są dane osobowe zawiera Załącznik Nr 1 do Polityki Bezpieczeństwa.

7.2 WYKAZ ZBIORÓW DANYCH OSOBOWYCH PRZETWARZANYCH W URZĘDZIE ORAZ SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY SYSTEMAMI

Wykaz zbiorów danych osobowych przetwarzanych w Urzędzie jest załącznikiem realizującym wymagania § 3 ust. 1 Rozporządzenia MSWiA (pkt. 1; 2; 3 i 4).

W załączniku znajdują się informacje dotyczące:

- wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych (jeżeli dane przetwarzane są w systemach informatycznych).
- opisu struktury zbiorów w przypadku (gdy producent oprogramowania nie dostarczył go w innej formie),
- sposobu przepływu danych pomiędzy systemami (jeżeli taki zachodzi).

Wykaz zbiorów danych osobowych przetwarzanych w Urzędzie Miejskim w Głownie stanowi załącznik nr 1 do Polityki Bezpieczeństwa

LP	Nazwa zbioru	Miejsce przetwarzania ze wskazaniem pomieszczeń	Aplikacja / System Papierowy	Opis przepływu danych pomiędzy systemami
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

7.3 PRZETWARZANIE DANYCH OSOBOWYCH

1. Dane osobowe w Urzędzie mogą być przetwarzane wyłącznie w pomieszczeniach wyznaczonych do przetwarzania danych osobowych.
2. Do pomieszczeń przetwarzania danych osobowych zalicza się:
   1) Pomieszczenia biurowe poszczególnych referatów, w których zlokalizowane są stacje robocze.
   2) Pomieszczenia, w których przechowywane są sprawne oraz uszkodzone elektroniczne nośniki informacji i kopie zapasowe.
   3) Pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego zawierające dane osobowe.
   4) Pomieszczenia, w których zlokalizowane są zbiory danych osobowych przetwarzanych w formie papierowej.
   5) Serwerownia.
3. Przebywanie wewnątrz obszarów, o których mowa w ust. 2, osób nieuprawnionych do przetwarzania danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych lub za zgodą ADO, który wydaje upoważnienie tymczasowe.
4. Budynki, pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób ograniczający możliwość dostępu do nich osobom nieupoważnionym.
5. Przetwarzanie danych osobowych jest zakazane w tych pomieszczeniach, w których osoby trzecie wykonują prace techniczne.
6. Nośniki elektroniczne zawierające dane osobowe należy przechowywać w zamykanych szafach, które znajdują się w obszarach przetwarzania danych osobowych.
7. Każdorazowe uchybienie zabezpieczeń fizycznych chroniących dane osobowe powinno być zgłaszane do ADO.

7.4 OPIS STRUKTURY DANYCH OSOBOWYCH WŁAŚCIWY DLA DANEGO ZBIORU DANYCH OSOBOWYCH PRZETWARZANEGO W URZĘDZIE

Opis struktury danych osobowych właściwy dla każdego zidentyfikowanego zbioru w Urzędzie zawiera się w załączniku nr 1 do polityki Bezpieczeństwa (pole: opis struktury).W przypadku, gdy istnieje dokument zewnętrzny opisujący strukturę danego zbioru Administrator Systemu zapewnia dostęp do właściwej dokumentacji technicznej dla aplikacji przetwarzającej dane osobowe danego zbioru. W przypadku, gdy Administrator Systemu nie posiada takich uprawnień, wskazuje jednostkę nadrzędną, właściwą w sprawie opisu struktury zbioru danych osobowych przetwarzanych w Urzędzie.

7.5 SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

ASI opisuje sposób przepływu danych pomiędzy poszczególnymi systemami. W przypadku, gdy ASI nie posiada takich uprawnień – wskazuje jednostkę nadrzędną, właściwą w sprawie opisu struktury zbioru danych osobowych przetwarzanych w Urzędzie.

Informacje odnośnie przepływu danych pomiędzy systemami zawarte są w odpowiednim polu w wykazie zbiorów danych osobowych (wzór w załączniku nr 1 do Polityki Bezpieczeństwa)

ROZDZIAŁ 8 UDOSTĘPNIANIE DANYCH OSOBOWYCH

a) Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie po akceptacji pisemnego wniosku skierowanego do ADO.

b) Udostępnienie danych osobowych na pisemny wniosek, może nastąpić przez pracowników poszczególnych Referatów Urzędu po wyrażeniu zgody przez ADO lub osoby przez niego upoważnionej z uprzednim zasięgnięciem opinii na temat zasadności udostępnienia danych od komórek merytorycznie właściwych.

c) ADO może odmówić udostępnienia danych, jeżeli może to naruszyć bezpieczeństwo i ochronę danych osobowych zgromadzonych w Systemie Informatycznym Urzędu.

ROZDZIAŁ 9 BEZPIECZEŃSTWO FIZYCZNE, TECHNICZNE I ORGANIZACYJNE

9.1 ŚRODKI FIZYCZNE

Do zastosowanych środków fizycznych w zakresie zabezpieczenia zbiorów danych osobowych przetwarzanych w Urzędzie należą w szczególności:

- zamykane na klucz pomieszczenia, w których przetwarzane są dane osobowe,
- zamykane na klucz szafy i szuflady w pokojach,
- zamykane na klucz okna na parterze budynku,
- system alarmowy,
- monitoring wejścia do urzędu i korytarza głównego,
- klimatyzacja w serwerowni jako zabezpieczenie ciągłości działania serwerów,
- sejf w serwerowni do zabezpieczenia nośników z kopiami zapasowymi danych.

9.2 ŚRODKI TECHNICZNE

Do zastosowanych środków technicznych użytych w celu zabezpieczenia zbiorów danych osobowych przetwarzanych w Urzędzie należą w szczególności:

- UPS'y,
- listwy przepięciowe,
- oprogramowanie AV,
- Firewall,
- wygaszacze ekranu,
- uwierzytelnianie do aplikacji i systemu,
- VPN,
- połączenia szyfrowane,
- kopie zapasowe.

9.3 ŚRODKI ORGANIZACYJNE

Do zastosowanych środków organizacyjnych użytych w celu zabezpieczenia zbiorów danych osobowych przetwarzanych w Urzędzie należą w szczególności (w całości lub poszczególne zapisy):

- Polityka bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Miejskim w Głownie,
- Instrukcja Zarządzania Systemem Informatycznym, służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Głownie,
- Regulamin organizacyjny Urzędu Miejskiego w Głownie,
- Regulamin pracy,
- Instrukcja p.poż.,
- lista osób upoważnionych do wchodzenia do Urzędu Miejskiego na podstawie indywidualnie nadawanych kodów,
- lista osób posiadających klucze do budynków Urzędu,
- konieczność każdorazowego zgłaszania firmie ochroniarskiej wejść i wyjść poza ustalonymi godzinami załączania i rozłączania alarmu (w ramach procedury ustalonej w umowie z agencją ochrony),
- Urząd posiada umowę z firmą ochroniarską na monitoring i interwencję w przypadku zadziałania alarmu,
- przebywanie w Urzędzie osób trzecich możliwe jest tylko w obecności osoby nadzorującej,
- osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych,

- przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego,
- w zakresach obowiązków pracownicy zobowiązują się do przestrzegania postanowień regulaminu pracy i ustalonego w zakładzie pracy porządku oraz przestrzegania tajemnicy określonej w odrębnych przepisach,
- osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,
- monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane,
- kopie zapasowe zbiorów danych osobowych przechowywane są na dysku sieciowym NAS (Network Attached Storage),
- pokoje zamykane są na klucz po zakończeniu pracy, klucze przechowywane są w zamykanej szafce przeznaczonej do tego celu.

ROZDZIAŁ 10 NARUSZENIE ZASAD OCHRONY

Za naruszenie bezpieczeństwa danych osobowych przetwarzanych za pomocą systemu informatycznego, uważa się każde zdarzenie lub działanie, łamiące zasady ochrony informacji, w szczególności takie, które może powodować utratę poufności, integralności lub ograniczenia dostępności do danych osobowych. Z każdego zdarzenia naruszającego bezpieczeństwo informacji osoby zgłaszające sporządzają notatkę służbową w sprawie dla ADO.

10.1 POSTĘPOWANIE W PRZYPADKACH WYSTĄPIENIA INCYDENTÓW ZWIĄZANYCH Z ZAGROŻENIEM BEZPIECZEŃSTWA DANYCH OSOBOWYCH PRZETWARZANYCH W URZĘDZIE.

1. Zakresem postępowania objęte są przypadki gdy:
   - stwierdzono naruszenie zabezpieczenia systemu informatycznego lub papierowego;
   - stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.
2. Użytkownik, który stwierdzi lub podejrzewa naruszenie zabezpieczenia lub złamanie zasad ochrony danych osobowych w systemie informatycznym lub papierowym Urzędu, niezwłocznie informuje o tym zdarzeniu ADO, a w przypadku naruszenia o charakterze informatycznym również ASI.
3. ADO we współpracy z ASI niezwłocznie podejmuje odpowiednie kroki w celu powstrzymania lub ograniczenia nieuprawnionego dostępu do danych osobowych przetwarzanych w Urzędzie, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów incydentu.
4. Po wyeliminowaniu bezpośredniego zagrożenia, ADO we współpracy z ASI przeprowadza analizę stanu systemu przetwarzania danych osobowych w celu potwierdzenia lub wykluczenia faktu naruszenia zasad bezpieczeństwa.
5. Jeżeli nastąpiło uszkodzenie zbioru danych, niezbędne jest jego odtworzenie z ostatniej kopii zapasowej z zachowaniem wszelkich środków ostrożności, mających na celu uniknięcia ponownego zdarzenia naruszającego bezpieczeństwo przetwarzanych danych.
6. Po przywróceniu stanu zapewniającego normalne funkcjonowanie ADO zarządza przeprowadzenie szczegółowej analizy w celu określenia przyczyn naruszenia zasad ochrony i/lub zabezpieczeń przetwarzanych w Urzędzie danych osobowych oraz w celu przedsięwzięcia kroków mających na celu wyeliminowanie podobnych zdarzeń w przyszłości.
   a) jeżeli przyczyną incydentu był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych w systemie informatycznym Urzędu, należy przeprowadzić dodatkowe szkolenie uwzględniając w szczególności zaistniały incydent;
   b) jeżeli przyczyną incydentu było uaktywnienie wirusa lub kodu szkodliwego, należy ustalić źródło jego pochodzenia oraz zapewnić dodatkowe zabezpieczenia mające na celu zminimalizowanie zagrożenia;
   c) jeżeli przyczyną incydentu było zaniedbanie ze strony osoby zatrudnionej przy przetwarzaniu danych osobowych w Urzędzie, należy wyciągnąć konsekwencje przewidziane przez przepisy karne Ustawy oraz rozważyć podjęcie sankcji dyscyplinarnych;

d) jeżeli przyczyną incydentu było włamanie w celu pozyskania zbioru danych osobowych lub jego części, należy dokonać szczegółowej analizy podjętych środków zabezpieczających, czy są one wystarczające i dobrać nowe jeżeli przeprowadzona analiza wykaże taką potrzebę;

e) jeżeli przyczyną incydentu był zły stan urządzenia lub sposób działania aplikacji, należy niezwłocznie przeprowadzić czynności dążące do przywrócenia odpowiedniego poziomu bezpieczeństwa aplikacji lub stanu technicznego urządzenia.

7. ADO zleca sporządzenie notatki, zawierającej informacje o przyczynach, przebiegu i wnioskach wyciągniętych w związku z zaistniałym incydentem (załączając ewentualne kopie dowodów dokumentujących to zdarzenie). Notatkę sporządza pracownik Referatu Organizacyjno – Administracyjnego. Sporządzoną notatkę załącza się do dokumentacji dotyczącej ochrony danych osobowych prowadzonej przez ADO.
8. Niezależnie od niniejszych zasad opisanych w Polityce bezpieczeństwa, w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych w Urzędzie.

10.2 SANKCJE W PRZYPADKU NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH.

1. Naruszenie zasad ochrony danych osobowych przez pracownika / wolontariusza / stażystę lub użytkownika zewnętrznego może skutkować postawieniem mu zarzutu popełnienia jednego z przestępstw określonych w Rozdziale 8 UODO lub przestępstwa określonego w art. 266 Kodeksu Karnego.
2. Zgodnie z art. 100 § 2 pkt 5 Kodeksu Pracy, pracownik jest obowiązany przestrzegać tajemnicy określonej w odrębnych przepisach. Dane osobowe, którym Urząd nadaje charakter poufny, mają charakter takiej tajemnicy, a jej ujawnienie w zależności od zakresu ujawnionych danych osobowych oraz nastawienia pracownika dopuszczającego się nieuprawnionego ujawnienia danych, może mieć charakter naruszenia lub ciężkiego naruszenia obowiązków pracowniczych.
3. Pracownik dopuszczający się nieuprawnionego ujawnienia lub wykorzystania danych osobowych w sposób sprzecznych z ich przeznaczeniem (np. wykorzystania danych osobowych do celów prywatnych) czy też ich przetwarzania w sposób niezgodny z przyjętymi w Urzędzie procedurami może zostać ukarany karą upomnienia lub karą nagany.
4. W razie ciężkiego naruszenia obowiązku zachowania danych osobowych w tajemnicy lub przetwarzania ich w sposób rażąco sprzeczny z przyjętymi zasadami i procedurami, ADO może rozwiązać bez wypowiedzenia umowę o pracę z winy pracownika.
5. Sankcje dotyczące ujawnienia poufnych danych osobowych stosuje się analogicznie do ujawnienia przez pracownika informacji dotyczących zabezpieczenia danych osobowych w Urzędzie.

ROZDZIAŁ 11 UPOWAŻNIENIA I SZKOLENIA

Osoby mające dostęp do danych osobowych przetwarzanych w Urzędzie powinny posiadać upoważnienie do przetwarzania danych osobowych (załącznik nr 4 do Polityki bezpieczeństwa) oraz zostać przeszkolone w zakresie przepisów dotyczących ochrony danych osobowych. Osoby, które zostały upoważnione do przetwarzania danych osobowych, są obowiązane zachować w tajemnicy wszelkie informacje dotyczące przetwarzania danych osobowych oraz sposobów ich zabezpieczania, z którymi zapoznały się podczas wykonywania obowiązków służbowych. Obowiązek ten nie wygasa w związku z ustaniem zatrudnienia.

Przed rozpoczęciem przetwarzania danych osobowych każdy pracownik powinien zostać przeszkolony. Szkolenie powinno obejmować następujące zagadnienia:

a. Przepisy o ochronie danych osobowych.
b. Zasady przetwarzania danych osobowych.
c. Procedury dotyczące bezpiecznego przetwarzania danych osobowych w systemach informatycznych Urzędu
d. Zasady użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych.
e. Zagrożenia na jakie może być narażone przetwarzanie danych osobowych, a w szczególności te związane z przetwarzaniem danych osobowych w systemach informatycznych.
f. Zasady dostępu do pomieszczeń, w których przetwarzane są dane osobowe.

g. Sposób postępowania w przypadku naruszenia ochrony danych osobowych (incydentów) lub systemu informatycznego.
h. Odpowiedzialność z tytułu naruszenia ochrony danych osobowych.

Szkolenia powinny być powtarzane okresowo lub na żądanie, gdy zaistnieje taka potrzeba.

ROZDZIAŁ 12 ZAŁĄCZNIKI:

1) **ZAŁĄCZNIK NR 1** - WYKAZ ZBIORÓW DANYCH OSOBOWYCH W URZĘDZIE MIEJSKIM W GŁOWNIE

2) **ZAŁĄCZNIK NR 2** – WZÓR REJESTRU OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH

3) **ZAŁĄCZNIK NR 3** – WZÓR WNIOSKU O NADANIE, POZBAWIENIE, MODYFIKACJĘ UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

4) **ZAŁĄCZNIK NR 4** – WZÓR UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

5) **ZAŁĄCZNIK NR 5** – WZÓR OŚWIADCZENIA PRACOWNIKA / WOLONTARIUSZA / STAŻYSTY / UŻYTKOWNIKA ZEWNĘTRZNEGO

Burmistrz Głowna
/-/
Grzegorz Janeczek

Wykaz zbiorów danych osobowych przetwarzanych w Urzędzie Miejskim w Głownie					
LP	**Nazwa zbioru**	**Miejsce przetwarzania ze wskazaniem pomieszczeń**	**Aplikacja / system papierowy**	**Opis przepływu danych pomiędzy systemami (jeżeli taki zachodzi)**	**Opis struktury zbioru (zakres przetwarzanych danych lub odwołanie do dokumentu zewnętrznego)**
1.	**EWIDENCJA LUDNOŚCI**	Referat Spraw Obywatelskich (I piętro budynku ul. Dworska 4 pok. 3)	Selwin – aplikacja/system papierowy	Dane mogą być eksportowane do pliku zewnętrznego (np. Excel, doc, csv itp.)	– Nazwiska i imiona – Data urodzenia – Miejsce urodzenia – Adres zamieszkania lub pobytu – PESEL – wykształcenie – Kod terytorialny – Rodzaj zameldowania, data zameldowania, data wymeldowania – Płeć – Nazwisko rodowe – Imię i nazwisko ojca (w tym nazwisko rodowe) – Imię matki – Nazwisko rodowe matki – Dane o urodzeniu (USC, kod terytorialny, numer aktu urodzenia oraz data wystawienia) – Stan cywilny, data zmiany, organ (kod terytorialny, nazwa organu, numer aktu) – Dane małżonka (nazwisko rodowe, imię, PESEL, forma ustania małżeństwa) – Dokument tożsamości (rodzaj, seria i numer, data wystawienia/ważności, wystawca: kod terytorialny, nazwa wystawcy) – Obowiązek wojskowy, dokument wojskowy: seria i numer, stopień wojskowy – Obywatelstwo obce (data zmiany) – Data zgonu – USC akt zgonu – Uprawnienia wyborcze – Status mieszkańca – Data wprowadzenia rekordu – Data ostatniej modyfikacji – Data przekroczenia granicy
2.	**SYSTEM WYDAWANIA DOWODÓW OSOBISTYCH**	Referat Spraw Obywatelskich (I piętro budynku ul. Dworska 4 pok. 3)	SWDO – aplikacja/system papierowy (koperty dowodowe)	Dane pobierane są i eksportowane drogą elektroniczną (osobne dedykowane łącze) do rejestrów MSWiA	– Nazwiska i imiona – Imiona rodziców – Data urodzenia – Miejsce urodzenia – Adres zamieszkania lub pobytu

					– PESEL – Seria i numer dowodu osobistego – Nazwisko rodowe – Nazwiska poprzednie – Nazwiska rodowe rodziców – Płeć – Rysopis (wzrost, kolor oczu, znaki szczególne) – Zdjęcie
3.	**REJESTRACJA I KWALIFIKACJA WOJSKOWA**	Referat Spraw Obywatelskich (parter budynku ul. Dworska 4 pok. 1)	Zbiór przetwarzany wyłącznie w formie papierowej	Brak przepływu danych	– Nazwisko i imię, – Imię ojca – Nazwisko rodowe – Data i miejsce urodzenia (rok, miesiąc, dzień) – Numer ewidencyjny PESEL – Seria i numer dowodu osobistego lub innego dokumentu – Miejsce aktualnego pobytu (stałego, czasowego ponad 2 miesiące) - miasto, ulica, numer domu i mieszkania) oraz dotychczasowe adresy zamieszkania, adres do korespondencji – Wezwano na dzień (rok, miesiąc, dzień) – Zgłosił się dnia (rok, miesiąc, dzień) – Uwagi
4.	**EWIDENCJA ŚWIADCZEŃ OSOBISTYCH I RZECZOWYCH**	Referat Spraw Obywatelskich (parter budynku ul. Dworska 4 pok. 1)	Zbiór przetwarzany wyłącznie w formie papierowej	Brak przepływu danych	– Imię i nazwisko – Adres zamieszkania – Zawód – Data urodzenia
5.	**OBRONA CYWILNA I ZARZĄDZANIE KRYZYSOWE**	Referat Spraw Obywatelskich (parter budynku ul. Dworska 4 pok. 1)	Zbiór przetwarzany wyłącznie w formie papierowej	Brak przepływu danych	– Imiona i nazwiska – Imiona rodziców – Data urodzenia – Adres zamieszkania lub pobytu – PESEL – Miejsce pracy – Zawód – Wykształcenie – Numer telefonu
6.	**SPRAWY OBRONNE**	Referat Spraw Obywatelskich (parter budynku ul. Dworska 4 pok. 1)	Zbiór przetwarzany wyłącznie w formie papierowej	Brak przepływu danych	– Imię nazwisko – Nazwisko rodowe – Adres – Wykształcenia – PESEL – Numer telefonu
7.	**WYKAZ LICENCJI NA PRZEWÓZ OSÓB TAKSÓWKĄ**	Referat Spraw Obywatelskich (I piętro	Zbiór przetwarzany wyłącznie w formie papierowej	Brak przepływu danych	– Imię i nazwisko – Adres

		budynku ul. Dworska 4 pok. 3)			– Numer licencji
8.	**OŚWIADCZENIA O STANIE MAJĄTKOWYM RADNYCH**	Biuro Rady Miejskiej (I piętro budynku ul. Dworska 4 pok. 4)	Zbiór przetwarzany wyłącznie w formie papierowej	Dane po zeskanowaniu i usunięciu informacji adresowych umieszczane są na BIP	– Miejscowość i dzień wypełnienia oświadczenia – Nazwisko i imię, nazwisko rodowe – Data i miejsce urodzenia – Miejsce zatrudnienia, stanowisko lub funkcja – Środki pieniężne zgromadzone w walucie obcej – Papiery wartościowe – Prowadzona działalność gospodarcza (forma prawna i przedmiot działalności) – Przychód i dochód osiągnięty z prowadzonej działalności gospodarczej – Zarządzana działalność gospodarcza (przedstawiciel, pełnomocnik, forma prawna, przedmiot działalności) – Dochód z zarządzania działalności gospodarczą – Działalność w spółkach handlowych (nazwa i siedziba spółki), czy jest członkiem zarządu (od kiedy), czy jest członkiem Rady nadzorczej (od kiedy),czy jest członkiem komisji rewizyjnej (od kiedy), dochody osiągnięte z tego tytułu – Działalność w fundacjach prowadzących działalność gospodarczą, czy jest członkiem zarządu (od kiedy), czy jest członkiem rady nadzorczej (od kiedy),czy jest członkiem komisji rewizyjnej (od kiedy, osiągnięte dochody) – Inne dochody z tytułu zatrudnienia lub innej działalności zarobkowej (z podaniem kwot uzyskiwanych z każdego tytułu) – Dom (powierzchnia, tytuł prawny, wartość) – Mieszkanie (powierzchnia, tytuł prawny, wartość) – Gospodarstwo rolne (rodzaj, powierzchnia , wartość, rodzaj zabudowy, tytuł prawny, dochód) – Inne nieruchomości (powierzchnia, tytuł prawny, wartość) – Udziały w spółkach handlowych (liczba, emitent udziałów, dochód) – Majątek nabyty od skarbu państwa, samorządu w drodze przetargu – Składki mienia ruchomego wartości powyżej 10.000 zł – Zobowiązania pieniężne o wartości powyżej 10.000 zł
9.	**AKTA STANU CYWILNEGO**	Urząd Stanu Cywilnego (parter budynku ul. Dworska 4 pok. 2)	Pb_usc – aplikacja / forma papierowa	Brak przepływu danych	– Nazwiska i imiona – Płeć, w przypadku zgłoszenia urodzenia dziecka – Data urodzenia – Miejsce urodzenia – Nazwisko rodowe – Stan cywilny – Miejsce zamieszkania – Data i miejsce zawarcia małżeństwa

					– Nazwisko noszone po zawarciu małżeństwa – Imiona i nazwiska rodziców (w tym nazwiska rodowe) – Ostatnie miejsce zamieszkania w przypadku zgonu osoby – Data zgonu, – Godzina zgonu – Miejsce zgonu – Data znalezienia zwłok, – Miejsce znalezienia zwłok – Przypiski – Zawód – Wykształcenie – PESEL – Seria i numer dowodu osobistego – Miejsce wydania dowodu osobistego – Miejsce wystawienia i numer aktu urodzenia żony/męża – Adnotacje o rozwodzie – Data unieważnienia aktu urodzenia/małżeństwa/zgonu – Imię nadane z urzędu – Data i numer orzeczenia sądu ustalającego ojcostwo, zaprzeczającego ojcostwo, przysposabiającego dziecko – Zmiana nazwiska dziecka – Data rozwiązania poprzedniego małżeństwa, rozwodu
10.	**Dane USC dla GUS**	Urząd Stanu Cywilnego (parter budynku ul. Dworska 4 pok. 2)	GUS APUSC3 - aplikacja	Dane przesyłane do GUS drogą elektroniczną	– Nazwisko, imiona – Nazwisko rodowe – Nazwiska poprzednie – PESEL – Data i miejsce urodzenia, małżeństwa, zgonu – Imiona i nazwiska rodowe rodziców – Seria i numer dowodu osobistego – Stan cywilny – Płeć – Adres zamieszkania
11.	**DZIENNIK KORESPONDENCYJNY**	Sekretariat I piętro budynku przy ul. Młynarskiej 15 pok. nr 6)	Zbiór przetwarzany wyłącznie w formie papierowej	Brak przepływu danych	– Imię i nazwisko lub nazwa nadawcy – Data wysłania – Data wpływu – Znak pisma – Informacja o sprawie – Komu zlecono załatwienie
12.	**UŻYTKOWNICY WIECZYŚCI, DZIERŻAWCY, NAJEMCY**	Referat Geodezji i Gospodarki Nieruchomościami (I piętro	Aplikacja Dzierżawcy Windows i aplikacja Użytkowanie Windows / forma papierowa	Przepływ danych pomiędzy wszystkimi aplikacjami firmy Proinfo.	– Imię i nazwisko – Seria i numer dowodu osobistego – PESEL

		przy ul. Młynarskiej 15 pok. nr 8, 9)		Możliwość eksportu do formatów zewnętrznych np. txt.	– Adres – Lokalizacja nieruchomości – Powierzchnia – Numer działki – Numer telefonu
13.	**DODATKI MIESZKANIOWE**	Archiwum zakładowe (pokój nr 17 w budynku przy ul. Młynarskiej 15)	Zbiór przetwarzany wyłącznie w formie papierowej	Brak przepływu danych	– Imię i nazwisko – Data urodzenia – PESEL – Dochody – Adres zamieszkania – Powierzchnia mieszkania – Ilość osób w gospodarstwie domowym – Wysokość czynszu
14.	**KADRY I PŁACE**	Referat Organizacyjno – Administracyjny (parter budynku przy ul Młynarskiej 15 pok. nr 3a) Referat Finansowo – Budżetowy (parter budynku przy ul. Młynarskiej 15 pok. nr 1, 3)	Aplikacja Płace Windows / forma papierowa	Przepływ danych za pomocą aplikacji Płatnik do Zakładu Ubezpieczeń Społecznych. Możliwość exportu do formatów zewnętrznych np. txt.	– Imię i nazwisko – Adres – Numer telefonu – NIP – PESEL – Seria i numer dowodu osobistego – Data urodzenia – Miejsce urodzenia – Imiona rodziców – Nazwisko rodowe – Nazwisko rodowe matki – Wykształcenie – Świadectwa pracy – Stan rodzinny – Imiona dzieci i małżonka ich daty urodzenia – Numer konta – Numer telefonu (pracownika / osoby do kontaktu w razie wypadku) – Informacje o powszechnym obowiązku obronnym (stosunek do powszechnego obowiązku obrony, stopień wojskowy, numer książeczki wojskowej, przynależność do WKU, przydział mobilizacyjny do sił zbrojnych RP)
15.	**PODATKI I OPŁATY LOKALNE**	Referat Finansowo – Budżetowy (parter budynku przy ul. Młynarskiej 15 pok. nr 1, 2, 3, 4)	Aplikacje Podatki Windows, Auta Windows, Oplok Windows, Kasa Windows, OPSKARB Windows, / forma papierowa	Przepływ danych pomiędzy wszystkimi aplikacjami firmy Proinfo. Możliwość eksportu do formatów zewnętrznych np. txt.	– Imię i nazwisko – Data urodzenia – Adres zamieszkania/pobytu – Imiona rodziców – REGON – NIP – PESEL – Rodzaj własności

					– Adresy nieruchomości – Powierzchnia nieruchomości – Dane pojazdu – Numer konta – Numer telefonu
16.	**PODATKI I OPŁATY LOKALNE – ROLNICTWO, LEŚNICTWO**	Referat Finansowo – Budżetowy (parter budynku przy ul. Młynarskiej 15 pok. nr 1)	Aplikacja Podatki Windows / forma papierowa	Przepływ danych pomiędzy wszystkimi aplikacjami firmy Proinfo. Możliwość eksportu do formatów zewnętrznych np. txt.	– Imię i nazwisko – Adres – REGON – NIP – PESEL – Rodzaj własności – Numer konta – Imiona rodziców – Adresy nieruchomości – Powierzchnia nieruchomości
17.	**ZAŚWIADCZENIA O POSIADANIU GOSPODARSTWA ROLNEGO ORAZ O WIELKOŚCI GOSPODARSTWA ROLNEGO**	Referat Finansowo – Budżetowy (parter budynku przy ul. Młynarskiej 15 pok. nr 1)	Zbiór przetwarzany wyłącznie w formie papierowej	Brak przepływu danych	– Imię i nazwisko – Adres zamieszkania wnioskodawcy – Lokalizacja nieruchomości – Powierzchnia – Rodzaj własności – Numer i seria dowodu osobistego – PESEL
18.	**STYPENDIA I ZASIŁKI SZKOLNE DLA UCZNIÓW**	Referat Oświaty i Infrastruktury Społecznej I piętro budynku przy ul. Ludwika Norblina 1, pok. 7 i 9	Zbiór przetwarzany wyłącznie w formie papierowej	Brak przepływu danych	– Imię i nazwisko – Data urodzenia – Adres zamieszkania lub pobytu wnioskodawcy – Nazwiska i imiona, daty urodzenia i stopień pokrewieństwa członków gospodarstwa domowego wnioskodawcy – Dochody – Numer ewidencyjny PESEL – Miejsce pracy – Numer telefonu – Numer rachunku bankowego
19.	**ZEZWOLENIA NA WYCINKĘ DRZEW**	Referat Ochrony Środowiska i Rolnictwa (I piętro budynku przy ul. Ludwika Norblina 1 pok. nr 18)	Zbiór przetwarzany wyłącznie w formie papierowej	Brak przepływu danych	– Nazwiska i imiona – Adres zamieszkania lub pobytu – Adres nieruchomości, na której zlokalizowane są drzewa lub krzewy do wycinki – Numer telefonu
20.	**DZIAŁALNOŚĆ GOSPODARCZA**	Referat Spraw Obywatelskich (I Piętro budynku ul. Dworska 4 pok. 3)	CEIDG online aplikacja / forma papierowa	Dane wprowadzane online do systemu CEIDG utrzymywane na serwerach CEIDG	– Nazwisko, imiona – Nazwisko rodowe – PESEL – Data i miejsce urodzenia

					– Seria i numer dowodu osobistego – Płeć – Adres zamieszkania – REGON – Rodzaj działalności gospodarczej
21.	**PŁATNIK**	Referat Finansowo – Budżetowy (parter budynku przy ul. Młynarskiej 15 pok. nr 1) Referat Organizacyjno – Administracyjny (parter budynku przy ul. Młynarskiej 15 pok. nr 3a)	Płatnik - aplikacja	Dane eksportowane drogą elektroniczną do ZUS	– Nazwisko, imiona – Nazwisko rodowe – Nazwiska poprzednie – PESEL – Data i miejsce urodzenia – Imiona i nazwiska, PESEL członków rodzin – Seria i numer dowodu osobistego – Numer książeczki wojskowej – Stan cywilny – Płeć – Adres zamieszkania – Obywatelstwo – Orzeczenie o niepełnosprawności
22.	**SYSTEM INFORMACJI OŚWIATOWEJ**	Referat Oświaty i Infrastruktury Społecznej I piętro budynku przy ul. Ludwika Norblina 1, pok. 7 i 9	SIO – aplikacja / forma papierowa	Dane eksportowane drogą elektroniczną i papierową do Kuratorium.	– Data urodzenia – Numer PESEL – Wykształcenie – Płeć – Formy i wymiar zatrudnienia – Stopień awansu zawodowego – Przygotowanie pedagogiczne – Formy kształcenia i doskonalenia – Sprawowane funkcje i zajmowane stanowiska – Rodzaj prowadzonych zajęć albo przyczyny nieprowadzenia zajęć – Staż pracy – Wysokość wynagrodzenia, z wyszczególnieniem jego składników – Wysokość dodatków
23.	**EWIDENCJA UMÓW NA ODBIÓR ODPADÓW KOMUNALNYCH OD WŁAŚCICIELI NIERUCHOMOŚCI**	Referat Ochrony Środowiska i Rolnictwa (I piętro budynku przy ul. Ludwika Norblina 1, pok. nr 18)	Zbiór przetwarzany wyłącznie w formie papierowej	Brak przepływu danych	– Nazwiska i imiona – Adres zamieszkania lub pobytu

24.	**OŚWIADCZENIA O STANIE MAJĄTKOWYM PRACOWNIKÓW I KIEROWNIKÓW MIEJSKICH JEDNOSTEK ORGANIZACYJNYCH**	Referat Organizacyjno – Administracyjny (parter budynku przy ul Młynarskiej 15, pok. nr 3a)	Zbiór przetwarzany wyłącznie w formie papierowej	Dane po zeskanowaniu i usunięciu informacji adresowych umieszczane są na BIP	– Miejscowość i dzień wypełnienia oświadczenia – Nazwisko i imię, nazwisko rodowe – Data i miejsce urodzenia – Miejsce zatrudnienia, stanowisko lub funkcja – Środki pieniężne zgromadzone w walucie obcej – Papiery wartościowe – Prowadzona działalność gospodarcza (forma prawna i przedmiot działalności) – Przychód i dochód osiągnięty z prowadzonej działalności gospodarczej – Zarządzana działalność gospodarcza (przedstawiciel , pełnomocnik, forma prawna , przedmiot działalności) – Dochód z zarządzania działalności gospodarczą – Działalność w spółkach handlowych (nazwa i siedziba spółki), czy jest członkiem zarządu (od kiedy), czy jest członkiem Rady nadzorczej (od kiedy), czy jest członkiem komisji rewizyjnej (od kiedy), dochody osiągnięte z tego tytułu – Działalność w fundacjach prowadzących działalność gospodarczą, czy jest członkiem zarządu (od kiedy), czy jest członkiem rady nadzorczej (od kiedy), czy jest członkiem komisji rewizyjnej (od kiedy), osiągnięte dochody – Inne dochody z tytułu zatrudnienia lub innej działalności zarobkowej (z podaniem kwot uzyskiwanych z każdego tytułu) – Dom (powierzchnia, tytuł prawny, wartość) – Mieszkanie (powierzchnia, tytuł prawny, wartość) – Gospodarstwo rolne (rodzaj , powierzchnia, wartość, rodzaj zabudowy, tytuł prawny, dochód) – Inne nieruchomości (powierzchnia, tytuł prawny, wartość) – Udziały w spółkach handlowych (liczba, emitent udziałów, dochód) – Majątek nabyty od skarbu państwa, samorządu w drodze przetargu – Składki mienia ruchomego wartości powyżej 10.000 zł – Zobowiązania pieniężne o wartości powyżej 10.000 zł
25.	**ZAŚWIADCZENIE O PRZEZNACZENIU TERENU W MIEJSCOWYM PLANIE ZAGOSPODAROWANIA PRZESTRZENNEGO**	Referat Geodezji i Gospodarki Nieruchomościami (I piętro budynku przy ul. Młynarskiej 15, pok. 8, 9)	Zbiory przetwarzane wyłącznie w formie papierowej	Brak przepływu danych	– Imię i nazwisko – Adres zamieszkania lub pobytu – Numer telefonu – Adres działki
26.	**WYPIS I WYRYS Z PLANU ZAGOSPODAROWANIA PRZESTRZENNEGO**	Referat Geodezji i Gospodarki Nieruchomościami (I piętro budynku przy ul.	Zbiory przetwarzane wyłącznie w formie papierowej	Brak przepływu danych	– Imię i nazwisko – Adres zamieszkania lub pobytu – Numer telefonu

		Młynarskiej 15, pok. 8, 9)			
27.	**REJESTR UMÓW**	Referat Organizacyjno – Administracyjny (parter budynku przy ul Młynarskiej 15 pok. nr 3a)	Zbiory przetwarzane wyłącznie w formie papierowej	Brak przepływu danych	– Imię i nazwisko – Adres zamieszkania – Numer i seria dowodu osobistego – PESEL – NIP
28.	**REJESTR UPOWAŻNIEŃ I PEŁNOMOCNICTW BURMISTRZA GŁOWNA**	Referat Organizacyjno – Administracyjny (parter budynku przy ul Młynarskiej 15 pok. nr 3a)	Zbiory przetwarzane wyłącznie w formie papierowej	Brak przepływu danych	– Imię i nazwisko – PESEL – Seria i numer dowodu osobistego – Numer upoważnienia
29.	**OSOBY ZGŁOSZONE JAKO UZALEŻNIONE I WSPÓŁUZALEŻNIONE DO GMINNEJ KOMISJI ROZWIĄZYWANIA PROBLEMÓW ALKOHOLOWYCH**	Referat Oświaty i Infrastruktury Społecznej I piętro budynku przy ul. Ludwika Norblina 1, pok. 7 i 9	Zbiory przetwarzane wyłącznie w formie papierowej	Brak przepływu danych	– Imię i nazwisko – Adres zamieszkania/pobytu – Numer PESEL – Data urodzenia – Stan zdrowia – Nałogi
30.	**ZEZWOLENIA NA SPRZEDAŻ NAPOJÓW ALKOHOLOWYCH**	Referat Oświaty i Infrastruktury Społecznej I piętro budynku przy ul. Ludwika Norblina 1, pok. 7 i 9	Aplikacja Oplok / forma papierowa	Przepływ danych pomiędzy wszystkimi aplikacjami firmy Proinfo. Możliwość eksportu do formatów zewnętrznych np. txt.	– Imię i nazwisko – Adres wnioskodawcy – Adres punktu sprzedaży – Nazwa punktu sprzedaży – NIP – PESEL
31.	**EWIDENCJA PLACÓWEK OŚWIATOWYCH NIEPUBLICZNYCH**	Referat Oświaty i Infrastruktury Społecznej I piętro budynku przy ul. Ludwika Norblina 1, pok. 7 i 9	Zbiory przetwarzane wyłącznie w formie papierowej	Brak przepływu danych	– Imię i nazwisko – Adres zamieszkania lub pobytu
32.	**AKTY AWANSU ZAWODOWEGO NAUCZYCIELI**	Referat Oświaty i Infrastruktury Społecznej I piętro budynku przy ul. Ludwika Norblina 1, pok. 7 i 9	Zbiory przetwarzane wyłącznie w formie papierowej	Brak przepływu danych	– Imię i nazwisko – Adres zamieszkania lub pobytu – Data urodzenia – Miejsce urodzenia – Wykształcenie – Numer telefonu – Staż pracy – Miejsce pracy

33.	**PRACOWNICY MŁODOCIANI**	Referat Oświaty i Infrastruktury Społecznej I piętro budynku przy ul. Ludwika Norblina 1, pok. 7 i 9	Zbiory przetwarzane wyłącznie w formie papierowej	Brak przepływu danych	– Imię i nazwisko – Adres zamieszkania lub pobytu – Data i miejsce urodzenia – PESEL – Nazwa placówki przyjmującej – Adres placówki przyjmującej – Wykształcenie – Zawód – Miejsce pracy – Wynagrodzenie
34.	**REJESTR SKARG I WNIOSKÓW**	Referat Organizacyjno – Administracyjny (parter budynku przy ul Młynarskiej 15 pok. nr 3a)	Zbiory przetwarzane wyłącznie w formie papierowej	Brak przepływu danych	– Imię i nazwisko – Adres zamieszkania lub pobytu
35.	**GOSPODARKA ODPADAMI**	Referat Ochrony Środowiska i Rolnictwa (parter budynku przy ul. Młynarskiej 15, pok. nr 4)	Aplikacja GOMIG – Odpady / forma papierowa	Przepływ danych pomiędzy aplikacją GOMIG – Odpady, a aplikacjami firmy Proinfo. Możliwość eksportu do formatów zewnętrznych np. txt.	– Imię i nazwisko – Adres zamieszkania lub pobytu – Numer telefonu – Adres nieruchomości na której powstają odpady komunalne – Rodzaj podmiotu składającego deklarację (właściciel nieruchomości, współwłaściciel nieruchomości, użytkownik wieczysty, zarządca lub użytkownik nieruchomości, inny podmiot władający nieruchomością)
36.	**ZWROT PODATKU AKCYZOWEGO**	Referat Ochrony Środowiska i Rolnictwa (parter budynku przy ul. Norblina 1, pok. nr 18)	Zbiór przetwarzany wyłącznie w formie papierowej	Brak przepływu danych	– Imię i nazwisko – NIP – PESEL – Seria i numer dowodu osobistego – Adres zamieszkania – Wielkość gospodarstwa rolnego – Numer konta bankowego
37.	**REJESTR MIESZKAŃCÓW I REJESTR CUDZOZIEMCÓW**	Referat Spraw Obywatelskich (I piętro budynku ul. Dworska 4 pok. 3)	System papierowy / aplikacja (osobne dedykowane łącze) do rejestrów MSWiA.	Dane są zbierane i wprowadzane do systemu ewidencji ludności i systemu dowodów osobistych prowadzonych przez MSWiA.	– Nazwiska i imiona – Data urodzenia – Miejsce urodzenia – Numer ewidencyjny PESEL – Nazwisko rodowe – Imiona i nazwiska rodowe rodziców – Kraj urodzenia – Stan cywilny – Oznaczenie aktu urodzenia i urzędy stanu cywilnego, w którym został on sporządzony – Peć – Obywatelstwo albo status bezpaństwowca – Imię i nazwisko rodowe oraz numer PESEL małżonka, jeżeli został mu

					nadany – Data zawarcia związku małżeńskiego, oznaczenie aktu małżeństwa i urzędu stanu cywilnego, w którym został on sporządzony, data rozwiązania związku małżeńskiego, sygnatura akt i oznaczenie sądu, który rozwiązał małżeństwo, sygnatura akt i oznaczenie sądu, który ustalił nieistnienie małżeństwa, sygnatura akt i oznaczenie sądu, który unieważnił małżeństwo, data zgonu małżonka albo data znalezienia jego zwłok, oznaczenie jego aktu zgonu i urzędu stanu cywilnego, w którym ten akt został sporządzony, – Adres i data zameldowania na pobyt stały; – Kraj miejsca zamieszkania, – Kraj poprzedniego miejsca zamieszkania, – Data wymeldowania z miejsca pobytu stałego, – Adres i data zameldowania na pobyt czasowy oraz data upływu deklarowanego terminu pobytu,\ – Data wymeldowania z miejsca pobytu czasowego, – Data wyjazdu poza granice Rzeczypospolitej Polskiej trwającego dłużej niż 6 miesięcy i wskazanie kraju wyjazdu, – Data powrotu z wyjazdu poza granice Rzeczypospolitej Polskiej trwającego dłużej niż 6 miesięcy, – Seria, numer i data ważności ostatniego wydanego dowodu osobistego obywatela polskiego oraz oznaczenie organu wydającego dokument, – Seria, numer i data ważności ostatniego wydanego paszportu obywatela polskiego, – Seria, numer i data ważności dokumentu podróży cudzoziemca, a w przypadku cudzoziemców, o których mowa w art. 7 ust. 1 pkt 3 lit a i b, ważnego dokumentu podróży lub innego ważnego dokumentu potwierdzającego tożsamość i obywatelstwo, – Data upływu deklarowanego przez cudzoziemca terminu pobytu, – Data zgonu albo data znalezienia zwłok, numer aktu zgonu i oznaczenie urzędu stanu cywilnego, w którym ten akt został sporządzony
38.	**PRZYDZIAŁ MIESZKAŃ**	Referat Infrastruktury Technicznej (I piętro budynku ul. Młynarskiej 15 pok. 10)	Zbiory przetwarzane wyłącznie w formie papierowej	Brak przepływu danych	– Imię i nazwisko wnioskodawcy – Adres zamieszkania wnioskodawcy – Imiona i nazwiska osób mających zamieszkać z wnioskodawcą – Data urodzenia osób mających zamieszkać z wnioskodawcą – Stosunek do wnioskodawcy – Data zameldowania – Właściciel lokalu – Tytuł prawny do zajmowanego lokalu – Dane o zajmowanym lokalu (powierzchnia, wyposażenie w urządzenia techniczne) – Liczba osób zameldowanych w miejscu zamieszkiwania

					współmałżonka (imię i nazwisko, rok urodzenia, stosunek pokrewieństwa) – Dochody
39.	**MONITORING WIZYJNY GMINY MIASTA GŁOWNO**	Referat Organizacyjno-Administracyjny (I piętro budynku przy ul. Młynarskiej 15, pok. 14)	Zbiór przetwarzany wyłącznie w formie elektronicznej – w formie nagrań wideo, przechowywanych lokalnie na serwerze przez maksymalnie 30 dni.	Brak przepływu danych.	– Dane dotyczące wizerunku osoby, – Numery rejestracyjne pojazdów
40.	**KONSULTACJE SPOŁECZNE**	Referat Oświaty i Infrastruktury Społecznej (I piętro budynku przy ul. Norblina 1, pok. 7)	„E- obywatelski" - aplikacja / forma papierowa	Brak przepływu danych	– Nazwiska i imiona – Data urodzenia – Adres zamieszkania – PESEL – Numer telefonu – Email
41.	**KARTA DUŻEJ RODZINY**	Miejski Ośrodek Pomocy Społecznej w Głownie (ul. Norblina 1, pok. 29 i 36)	Aplikacja SI KDR/forma papierowa	Dane są eksportowane drogą elektroniczną do Państwowej Wytwórni Papierów Wartościowych	– Nazwiska i imiona, – Imiona rodziców, – Data urodzenia, – Adres zamieszkania lub pobytu, – Numer ewidencyjny PESEL, – Numer telefonu, – Nazwiska rodowe rodziców dziecka, – Informacje o zgonie, – Adres do korespondencji, – Numer dokumentu potwierdzającego tożsamość w przypadku osób, które nie posiadają numeru PESEL, – Stan cywilny, – Obywatelstwo, – Stopień pokrewieństwa z członkami rodziny, – Informacje o uczęszczaniu dziecka do szkół i placówek oświatowych, o których mowa w art. 3 ust. 1 pkt 1 ustawy z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej (Dz. U. z 2016 r. poz. 1927 i 1984 oraz z 2017 r. poz. 60 i 777), okresie uczęszczania, typie lub rodzaju instytucji oraz nazwie i adresie siedziby instytucji, do której dziecko uczęszcza, – Informacje o uczęszczaniu dziecka do szkoły wyższej, okresie uczęszczania oraz nazwie i adresie siedziby szkoły wyższej, do której dziecko uczęszcza, – informację o umieszczeniu dziecka w pieczy zastępczej, – dochody członków rodziny wielodzietnej - w przypadku złożenia wniosku, o którym mowa w art. 13 ust. 3, – adres poczty elektronicznej członka rodziny wielodzietnej, – informacje o zawarciu, rozwiązaniu przez rozwód, unieważnieniu lub stwierdzeniu przez sąd nieistnienia związku małżeńskiego,

					– informacje o znacznym lub umiarkowanym stopniu niepełnosprawności, w tym informacje o okresie, na jaki zostało wydane orzeczenie o znacznym lub umiarkowanym stopniu niepełnosprawności, – orzeczenie sądu o odebraniu lub ograniczeniu władzy rodzicielskiej
42.	**PLAN WYDAWANIA TABLETEK JODKU POTASU**	Referat Spraw Obywatelskich (parter budynku przy ul. Dworskiej 4, pok. nr 1)	Zbiór przetwarzany wyłącznie w formie papierowej	Brak przepływu danych	– imię i nazwisko, – adres zamieszkania lub pobytu, – miejsce pracy, – numer telefonu
43.	**ZAKŁADOWY FUNDUSZ ŚWIADCZEŃ SOCJALNYCH**	Referat Organizacyjno Administracyjny (parter budynku przy ul. Młynarskiej 15, pok. nr 3a)	Zbiór przetwarzany wyłącznie w formie papierowej	Brak przepływu danych	– Imię i nazwisko, – Adres zamieszkania, – Imiona i nazwiska członków rodziny wspólnie zamieszkujących i prowadzących wspólne gospodarstwo domowe, stopień pokrewieństwa, data urodzenia, miejsce pracy lub nazwa szkoły, orzeczenie o niepełnosprawności, – Miesięczny dochód na osobę w rodzinie

Burmistrz Głowna

/-/

Grzegorz Janeczek

REJESTR OSÓB UPOWAŻNIONYCH PRZEZ ADMINISTRATORA DANYCH OSOBOWYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Nr upoważnienia	Nazwisko i imię	Stanowisko	Nazwa zbioru danych osobowych (zgodna z zał. nr 1)	Zakres przetwarzania	Udzielono od - do	Identyfikator

Legenda:
PZ- Pełen zakres, **Z** – zbierania, **U** – utrwalania, **O** – opracowywania, **W** – wprowadzania, **P** – przechowywania, **Us** – usuwania, **Ud** – udostępniania, **M** – modyfikacji, **Po** – podglądu

Burmistrz Głowna
/-/
Grzegorz Janeczek

…… ……..……..…….
(dnia) (nazwa komórki organizacyjnej)

WNIOSEK

Zgodnie z art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych
(t.j. Dz. U. z 2016 r. poz. 922)

Wnioskuję o nadanie / pozbawienie / zmianę / *

Pani / Panu ……..……
Stanowisko …….…….

upoważnienia ……..do przetwarzania danych osobowych w Urzędzie Miejskim w Głownie.
(Nr upoważnienia w przypadku wniosku o modyfikację lub odebranie)

Upoważnienie wydaje się na okres: stały / czasowy – do kiedy/* ……..

1. Nazwa zbioru danych osobowych ze wskazaniem zakresu przetwarzania danych w zbiorze**:
…….
……
……
……
……
……
……
……
……
……
……
……

3. Sposób przetwarzania danych osobowych: papierowy / informatyczny*

4. Wnioskuję o nadanie identyfikatora i hasła do systemu informatycznego: tak / nie *

5. Osoba została zapoznana z przepisami o ochronie danych osobowych: tak / nie *

……..
(podpis przełożonego/kierownika referatu)

*- niepotrzebne skreślić
** - Pz – pełen zakres, Z-zbierania, U-utrwalania, O-opracowywania, W-wprowadzania, P- przechowywania, Us- usuwania, Ud- udostępniania, M-modyfikacji, Po-podglądu

Załącznik Nr 4 do Polityki Bezpieczeństwa

Głowno, dnia .....

UPOWAŻNIENIE Nr ..../.....

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych
(t.j. Dz. U. z 2016 r. poz. 922)

upoważniam

Pana/Panią:

zatrudnionego/zatrudnioną na stanowisku:

do przetwarzania danych osobowych w zbiorze/zbiorach o nazwie:

Nazwa zbioru	Sposób przetwarzania danych*	Identyfikator *	Zakres przetwarzania danych*

**(tradycyjny (papierowy)/informatyczny)*
**(w przypadku przetwarzania danych w systemie informatycznym)*
**(Pz - pełen zakres; Z – zbierania; U – utrwalania; O – opracowywania; W – wprowadzania; P – przechowywania; Us – usuwania; Ud – udostępniania; M – modyfikacji; Po - podglądu)*

Upoważnienie wydaje się na okres .....

Jednocześnie zobowiązuję Pana/Panią do przestrzegania przepisów dotyczących ochrony danych osobowych zawartych w cytowanej wyżej ustawie z dnia 29 sierpnia 1997 r.

…….
(podpis Administratora Danych Osobowych)

Przyjmuję do wiadomości i przestrzegania,
zobowiązuję się do zachowania w tajemnicy
tych danych oraz sposobów ich zabezpieczeń.

……
(data i podpis pracownika)

…… ……..……..…….
(data) (imię i nazwisko pracownika / wolontariusza / stażysty / użytkownika zewnętrznego) *

Oświadczenie pracownika / wolontariusza / stażysty / użytkownika zewnętrznego* dopuszczonego do przetwarzania danych osobowych w zbiorach danych przetwarzanych przez Urząd Miejski w Głownie

I. Obowiązki pracownika / wolontariusza / stażysty / użytkownika zewnętrznego *

Pracownik / wolontariusz/ stażysta/ użytkownik zewnętrzny* dopuszczony do przetwarzania danych osobowych zobowiązany jest do:

1. Zapoznania się i przestrzegania obowiązków wynikających z:
   a) Przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922) oraz aktów wykonawczych wydanych na jej podstawie,
   b) Dokumentów wprowadzonych przez Urząd Miejski w Głownie w związku z przetwarzaniem danych osobowych, w szczególności:
      - Polityki Bezpieczeństwa Przetwarzania Danych Osobowych Urzędu Miejskiego w Głownie,
      - Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych.

2. Zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem.

3. Zachowania w tajemnicy danych oraz sposobu ich zabezpieczenia do których uzyskał dostęp w upoważnieniu, również po jego wygaśnięciu.

II. Odpowiedzialność pracownika

1. Za niedopełnienie obowiązków wynikających z niniejszego oświadczenia osoba upoważniona ponosi odpowiedzialność na podstawie przepisów Kodeksu Karnego, Regulaminu pracy oraz Ustawy o ochronie danych osobowych.

Oświadczam, że treść niniejszego oświadczenia jest mi znana

i zobowiązuję się do jego przestrzegania.

Potwierdzam odbiór jednego oświadczenia.

…….. ……

Pracownik / wolontariusz / stażysta / użytkownik zewnętrzny* Administrator Danych Osobowych

*-niepotrzebne śkreślić

Załącznik Nr 2
do Zarządzenia 164/2017
Burmistrza Głowna
z dnia 27 listopada 2017 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE MIEJSKIM W GŁOWNIE

SPIS TREŚCI

ROZDZIAŁ 1 WYKAZ SKRÓTÓW I DEFINICJI

SKRÓTY	
UODO	Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
Rozporządzenie MSWiA	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie sposobu przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
Urząd	Urząd Miejski w Głownie ul. Młynarska 15, 95-015 Głowno (wraz z innymi lokalizacjami).
ADO	Administrator Danych Osobowych w Urzędzie Miejskim w Głownie.
ASI/ Informatyk Urzędu	Administrator Systemu/ Administrator Systemu Informatycznego – Starszy Informatyk w Urzędzie Miejskim w Głownie.
Polityka bezpieczeństwa	Polityka bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Miejskim w Głownie.
Instrukcja	Instrukcja zarządzania systemem informatycznym w Urzędzie Miejskim w Głownie.
GIODO	Generalny Inspektor Ochrony Danych Osobowych

DEFINICJE	
Administrator Danych Osobowych	Podmiot decydujący o celach i środkach przetwarzania danych osobowych w Urzędzie – Burmistrz Głowna.
Administrator Systemów Informatycznych	Pracownik Urzędu wyznaczony przez Burmistrza (ADO), odpowiedzialny za funkcjonowanie infrastruktury informatycznej oraz za stosowanie technicznych środków bezpieczeństwa w tych systemach – **Informatyk Urzędu.**
Dane osobowe	Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
Zbiór danych osobowych	Każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów
Użytkownik	Osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym Urzędu i posiadająca w nim aktywny profil użytkownika zabezpieczony hasłem dostępu. Użytkownikiem może być pracownik Urzędu, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż lub praktyki w Urzędzie, jeżeli posiada stosowne upoważnienie do przetwarzania danych osobowych.
Osoba uprawniona/ upoważniona	Każda osoba posiadająca ważne upoważnienie do przetwarzania danych osobowych nadane przez ADO.
System informatyczny	Zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
Przetwarzanie danych	Jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach Informatycznych.
Sieć lokalna	Połączenie systemów informatycznych Urzędu wyłącznie dla własnych jego potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.
Sieć publiczna	Sieć publiczna w rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907 z późn. zm.)

Identyfikator Użytkownika	Ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
Zabezpieczenie danych osobowych	Środki organizacyjne, techniczne i fizyczne wdrożone w celu zabezpieczenia zasobów technicznych oraz ochrony przed zniszczeniem, nieuprawnionym dostępem i modyfikacją, ujawnieniem lub pozyskaniem danych osobowych bądź ich utratą.
Integralność danych	Właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
Poufność danych	Właściwość zapewniająca, że dane osobowe nie są udostępniane nieupoważnionym osobom.
Dostępność	Właściwość zapewniająca, że dane osobowe są dostępne dla wszystkich upoważnionych osób.
Stacja robocza	Komputer / laptop wraz z oprogramowaniem będący elementem systemu informatycznego służącego do przetwarzania danych osobowych w Urzędzie Miejskim w Głownie za pomocą którego użytkownik wykonuje swoje obowiązki służbowe.

ROZDZIAŁ 2 CEL INSTRUKCJI ZARZĄDZANIA SYSTEMEM

Celem opracowania Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Głownie jest określenie zasad zarządzania i zabezpieczania systemu zgodnie z wymaganiami określonymi w rozporządzeniu MSWiA. Ochronie podlegają dane, jednostki robocze, i inny sprzęt, systemy operacyjne i informatyczne oraz pomieszczenia, w których odbywa się proces przetwarzania danych osobowych. Zamieszczone w Instrukcji zapisy mają na celu ochronę danych osobowych, przetwarzanych w Urzędzie, przed udostępnieniem ich osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem danych z naruszeniem przepisów Ustawy o ochronie danych osobowych, nieuprawnioną zmianą danych, ich utratą, uszkodzeniem lub zniszczeniem.

ROZDZIAŁ 3 ZAKRES I WARUNKI STOSOWANIA DOKUMENTU

Niniejsza instrukcja dotyczy każdego zbioru danych osobowych przetwarzanego w Urzędzie zarówno w formie elektronicznej jak i papierowej.

Aktualny wykaz przetwarzanych zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, ich lokalizacją i sposobem dostępu znajduje się w Załączniku 1 do Polityki bezpieczeństwa.

ROZDZIAŁ 4 ODPOWIEDZIALNOŚĆ

Dokument jest dedykowany wszystkim osobom i podmiotom odpowiedzialnym za prawidłowe funkcjonowanie systemu informatycznego Urzędu oraz za jego eksploatację.

Za przestrzeganie zasad wymienionych w niniejszej instrukcji odpowiadają poszczególne podmioty:

a) **Administrator Danych Osobowych** – realizujący zadania w zakresie objęcia nadzorem czynności wykonywanych zgodnie z niniejszą Instrukcją.
b) **Administrator Systemu/ Administrator Systemu Informatycznego** – Informatyk Urzędu realizujący zadania w zakresie zapewnienia konfiguracji systemu informatycznego zgodnie z wymaganiami wynikającymi z niniejszej Instrukcji, a także przeprowadzania postępowań kontrolnych w zakresie przestrzegania zasad i obowiązków ich stosowania.
c) **Użytkownicy systemu w zakresie wykonywania czynności objętych niniejszą Instrukcją**.

ROZDZIAŁ 5 NADAWANIE UPRAWNIEŃ DO PRZETWARZANIA DANYCH W SYSTEMIE INFORMATYCZNYM URZĘDU

5.1 NADAWANIE COFANIE I MODYFIKACJA UPRAWNIEŃ DO PRZETWARZANIA DANYCH W SYSTEMIE INFORMATYCZNYM URZĘDU

a) Przetwarzać dane osobowe w systemie informatycznym Urzędu może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych (wzór upoważnienia stanowi załącznik nr 4 do Polityki bezpieczeństwa).

b) Wydanie upoważnienia oraz rejestracja użytkownika systemu informatycznego przetwarzającego dane osobowe następuje na wniosek Kierownika Referatu / osoby sprawującej nadzór nad komórką organizacyjną.

c) ASI na podstawie upoważnienia nadaje Użytkownikom odpowiednie uprawnienia w systemie informatycznym, zgodnie z zakresem przyznanego Upoważnienia do przetwarzania danych osobowych.

d) Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla użytkownika identyfikatora jednoznacznie identyfikującego go w systemie i nadanie mu hasła oraz zakresu dostępnych dla niego danych i operacji zgodnych ze stanowiskiem pracy.

e) Hasło ustanowione podczas nadawania uprawnienia dostępu do systemu informatycznego Urzędu przez ASI należy zmienić na indywidualne podczas pierwszego logowania.

f) Ustanowione hasło, ASI przekazuje użytkownikowi ustnie lub mailowo na jego indywidualne konto (zabezpieczone hasłem dostępu). Poprzez logowanie do systemu rozumie się uwierzytelnianie w grupie roboczej / domenie do której przypisany jest użytkownik systemu informatycznego oraz aplikacjach dedykowanych służących do przetwarzania danych osobowych w Urzędzie.

g) Użytkownik ma obowiązek przestrzegania zasad eksploatacji systemów informatycznych, wykorzystywanych do przetwarzania danych osobowych w Urzędzie i realizacji związanych z tym procedur. Użytkownik ma prawo do wykonywania w systemie informatycznym Urzędu jedynie tych czynności, które wynikają z powierzonych mu zadań i nadanych uprawnień.

h) Użytkownik jest odpowiedzialny za wszystkie wykonywane operacje w systemie informatycznym Urzędu wykonane przy użyciu jego identyfikatora.

i) Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień, jak również próba złamania funkcjonujących w systemie informatycznym mechanizmów ochronnych są niedozwolone i podlegają sankcjom dyscyplinarnym (a w przypadku naruszenia przepisów o ochronie danych osobowych również karnym).

j) Bezpośredni przełożony użytkownika ma obowiązek poinformować ASI o konieczności cofnięcia uprawnień w systemie informatycznym Urzędu. ASI na podstawie zgłoszenia bezzwłocznie cofa uprawnienia danemu użytkownikowi.

k) W przypadku konieczności modyfikacji (zmiany/ rozszerzenia/ zwężenia) zakresu uprawnień, potrzebę zmiany zgłasza bezpośredni przełożony Użytkownika. ASI na podstawie zgłoszenia bezzwłocznie dokonuje stosownej modyfikacji.

l) Za bezpieczeństwo danych osobowych w użytkowanych systemach informatycznych w trybie bezpośredniej realizacji (wykonawstwo) odpowiedzialni są wszyscy użytkownicy w zakresie realizowanych przez siebie

zadań i czynności, związanych z przetwarzaniem danych osobowych, które wynikają z pisemnego upoważnienia do przetwarzania danych osobowych.

5.2 REJESTROWANIE UPRAWNIEŃ

a) Dla każdego użytkownika systemu informatycznego Urzędu, któremu zostało nadane upoważnienie do przetwarzania danych osobowy ustala się identyfikator, który podlega zarejestrowaniu w systemie informatycznym wraz z imieniem i nazwiskiem użytkownika. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu nie może być przydzielany innej osobie. Użytkownik otrzymuje od ASI hasło inicjujące (zmieniane osobiście przy pierwszym logowaniu) oraz indywidualny zakres uprawnień w systemie.

b) Rejestracja uprawnień posiadanych dla każdego użytkownika systemu informatycznego, służącego do przetwarzania danych osobowych w Urzędzie, wykonywana jest za pomocą Rejestru osób upoważnionych prowadzonego w Referacie Organizacyjno – Administracyjnym - załącznik nr 2 do Polityki bezpieczeństwa.

ROZDZIAŁ 6 ŚRODKI I METODY UWIERZYTELNIANIA UŻYTKOWNIKÓW W SYSTEMIE

6.1 UWIERZYTELNIANIE W SYSTEMIE INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH.

a) W systemie informatycznym służącym do przetwarzania danych osobowych w Urzędzie stosuje się trzyetapowe uwierzytelnianie:
   - na poziomie dostępu do jednostki roboczej poszczególnych użytkowników,
   - na poziomie dostępu do poszczególnych aplikacji za pomocą których przetwarzane są zbiory danych osobowych w Urzędzie,
   - na poziomie dostępu administratora.

b) Bezpośredni dostęp do aplikacji przetwarzającej dane osobowe w systemie informatycznym Urzędu może mieć miejsce wyłącznie po uwierzytelnieniu użytkownika poprzez podanie przez niego prawidłowego identyfikatora oraz właściwego hasła dostępu (na poziomie dostępu do systemu operacyjnego i na poziomie dostępu do aplikacji).

c) W przypadku przetwarzania danych osobowych w zbiorach za pomocą aplikacji do których nie ma możliwości uwierzytelniania (m. in. typu: Word, Excel) – użytkownik zobowiązany jest zabezpieczyć taki zbiór hasłem dostępu zgodnie z zasadami posługiwania się hasłami opisanymi w niniejszym dokumencie.

d) ASI posiada własne konto administracyjne w systemie informatycznym, do którego ma przydzielone hasło. Zasady zarządzania hasłami ASI są analogiczne, jak w przypadku haseł użytkowników.

e) Identyfikator i hasło użytkowników posiadających uprawnienia administratorów systemów informatycznych powinny być przechowywane w zamkniętym sejfie zlokalizowanym w serwerowni Urzędu Miejskiego w Głownie ul. Młynarska 15, do którego dostęp jest w pełni kontrolowany, przy czym dostęp mają wyłącznie uprawnione osoby. Nazwy użytkowników oraz hasła powinny być przechowywane w opieczętowanej i opatrzonej podpisem ASI kopercie.

f) W przypadku konieczności awaryjnego użycia identyfikatora i hasła awaryjnego konieczne jest sporządzenie notatki na ten temat.

g) Notatka powinna zawierać następujące informacje:
   - dane osoby upoważnionej do otwarcia koperty z identyfikatorem i hasłem awaryjnym,
   - dane i stanowisko osoby, wykonującej czynności za pomocą identyfikatora i hasła awaryjnego, jeżeli jest inna od osoby pobierającej,

- krótki opis sytuacji, która spowodowała konieczność awaryjnego wykorzystania identyfikatora i hasła awaryjnego.

h) O konieczności i okolicznościach awaryjnego użycia nazw i haseł musi niezwłocznie zostać powiadomiony ASI.

6.2 ZASADY POSŁUGIWANIA SIĘ HASŁAMI

a) Hasło użytkownika musi być zmieniane przez użytkownika co najmniej raz na 30 dni.

b) Identyfikator użytkownika nie powinien być zmieniany bez uzasadnionej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.

c) Użytkownicy są odpowiedzialni za zachowanie poufności swoich haseł.

d) Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.

e) Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.

f) W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, użytkownik zobowiązany jest do natychmiastowej jego zmiany.

g) Przy wyborze hasła obowiązują następujące zasady:

- minimalna długość hasła: 8 znaków w tym: wielkie litery, cyfry lub znaki specjalne,
- zakazuje się stosować:
  - haseł, które użytkownik stosował uprzednio przez okres 3 miesięcy,
  - swojej nazwy użytkownika, imion, nazwisk, funkcji, komórki organizacyjnej, itd.,
  - ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy na której mieszka lub pracuje, itp.,
  - nazw własnych,
  - sekwencji znaków z klawiatury np.: QWERTY", "12345678",itp.
- należy stosować:
  - hasła zawierające kombinacje liter i cyfr lub znaków specjalnych,
  - hasła, które można zapamiętać bez zapisywania,
  - hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim.

h) Zmienionego hasła nie wolno powierzać innym osobom.

i) W systemach, które umożliwiają opcję zapamiętania nazw użytkownika lub jego hasła nie należy korzystać z takiej możliwości.

ROZDZIAŁ 7 ROZPOCZYNANIE, ZAWIESZANIE I KOŃCZENIE PRACY W SYSTEMIE

7.1 ZASADY ROZPOCZĘCIA PRACY W SYSTEMIE

a) Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każdy użytkownik obowiązany jest do zwrócenia uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych.

b) Szczegółowy opis takich symptomów oraz sposób postępowania w przypadku ich wykrycia został opisany w rozdziale 10 Polityki bezpieczeństwa.

c) Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.

d) Pięciokrotne błędne wprowadzenie hasła powoduje zablokowanie dostępu do systemu lub aplikacji (w przypadku aplikacji umożliwiających taka procedurę) i konieczność zgłoszenia tego faktu ASI.

7.2 ZASADY ZAWIESZENIA PRACY W SYSTEMIE

a) W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 15 minut automatycznie włączany jest wygaszacz ekranu. Wygaszacze ekranu powinny być zaopatrzone w hasła zbudowane analogicznie do haseł używanych przez użytkownika przy logowaniu. Hasło powinno składać się z co najmniej 8 znaków, powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne oraz być zmieniane nie rzadziej niż co 30 dni.

b) Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest, aby dwóch lub większa ilość użytkowników wykorzystywała wspólnie jedno konto użytkownika.

c) W przypadku, gdy użytkownik odchodzi od stacji roboczej lub przerywa na niej pracę na dłużej niż 60 minut zobowiązany jest wylogować się z aplikacji i systemu stacji roboczej, na której pracuje oraz sprawdzić czy nie zostały pozostawione bez zamknięcia nośniki informacji zawierające dane osobowe.

d) W pomieszczeniach, w których przetwarzane są dane i w których jednocześnie mogą przebywać osoby postronne, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane.

e) W trakcie pracy użytkownika, wszelkie dokumenty zawierające dane osobowe powinny być przechowywane w taki sposób, aby uniemożliwić wgląd w nie osobom nieuprawnionym. Wydruki zawierające dane osobowe należy zniszczyć w przypadku, w którym nie są już potrzebne lub zarchiwizować w przypadku, gdy są niezbędne dla prawidłowej realizacji czynności służbowych przez osoby uprawnione.

f) Niedopuszczalne jest na służbowym stanowisku pracy odwiedzanie i pobieranie danych z nieautoryzowanych witryn internetowych o treści niezwiązanej z działalnością Urzędu a zwłaszcza w celach prywatnych.

g) Ujawnione przypadki stwierdzenia nieprawidłowości działania systemu należy zgłaszać do ADO/ASI.

h) W przypadku przerwy w dostawie energii elektrycznej należy jak najszybciej zakończyć pracę w systemie informatycznym, tak aby możliwe było bezpieczne zamknięcie aplikacji i zapisanie efektów pracy użytkowników (w przypadku gdy stacje robocze posiadają zapasowe źródło zasilania).

i) Gdy zasilanie elektryczne zostanie przywrócone, należy poczekać 10 minut przed ponownym uruchomieniem urządzeń tak, aby zmniejszyć ryzyko uruchomienia systemu w okresie niestabilnego zasilania.

7.3 ZASADY ZAKOŃCZENIA PRACY W SYSTEMIE

a) Przed wyłączeniem Stacji roboczej należy bezwzględnie zakończyć pracę uruchomionych programów, wyłączyć się z użytkowanych zasobów sieci komputerowej.

b) Niedopuszczalne jest wyłączanie komputera z pominięciem procedur zamknięcia oprogramowania oraz zakończeniem pracy w sieci.

c) Zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika z aplikacji.

ROZDZIAŁ 8 TWORZENIE KOPII ZAPASOWYCH I NOŚNIKÓW INFORMACJI

8.1 KOPIE ZAPASOWE SYSTEMU INFORMATYCZNEGO, ZA WYKONYWANIE KTÓRYCH ODPOWIEDZIALNY JEST ASI

a) Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada ASI.

b) Kopie zapasowe informacji przechowywanych w systemie informatycznym przetwarzającym dane osobowe tworzone są w następujący sposób:

- wykonuje się kopie całościowe,

- kopia danych finansowych oraz pozostałych danych wykonywana jest raz dziennie przy użyciu streamera oraz przy pomocy serwera NAS (Network Attached Storage),

- do wykonywania kopi zapasowych wykorzystuje się oprogramowanie przeznaczone do wykonywania bekapu,

c) Miejscem wykonywania kopii zapasowych jest siedziba Urzędu Miejskiego w Głownie oraz poszczególne jej lokalizacje.

d) Kopie wykonywane dla danych gromadzonych przez użytkowników wykonywane są na wyznaczonym udziale dysku na serwerze plików, dostępnym dla każdego upoważnionego użytkownika w celu gromadzenia tam, zgodnie z określoną strukturą, danych osobowych oraz innych danych mających istotny wpływ dla ciągłości działania Urzędu.

e) ASI wykonując kopię zapasową zobowiązany jest do przetestowania nośnika na którym wykonano kopię w zakresie integralności i możliwości odtworzenia zapisanych tam danych.

8.2 KOPIE ZAPASOWE SYSTEMU INFORMATYCZNEGO, ZA WYKONYWANIE KTÓRYCH ODPOWIEDZIALNI SĄ UŻYTKOWNICY

W przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych użytkownicy systemu informatycznego zobowiązani są do centralnego przechowywania kopii danych, tak aby możliwe było zabezpieczenie ich dostępności poprzez wykonanie kopii zapasowych.

8.3 PRZECHOWYWANIE KOPII ZAPASOWYCH

a) W przypadku przechowywania kopii zapasowych przez okres dłuższy niż pół roku, wszystkie kopie zapasowe zbiorów danych osobowych, aplikacji przetwarzających dane osobowe oraz danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, których to dotyczy muszą być okresowo (co najmniej raz na pół roku) sprawdzane pod względem ich dalszej przydatności. Czynności te wykonuje ASI.

b) Nośniki kopii zapasowych, które zostały wycofane z użycia, jeżeli jest to możliwe, należy pozbawić zapisanych danych za pomocą oprogramowania do bezpiecznego usuwania zapisanych danych. W przeciwnym wypadku podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika, w sposób uniemożliwiający odczytanie zapisanych na nich danych.

c) Nośniki zawierające kopie zapasowe są wyraźnie oznaczone z podaniem daty wykonania kopii i jej zakres (kopia całościowa lub określony wzór).

d) Nośniki, za pomocą których utworzone zostały kopie zapasowe przechowywane są w serwerowni Urzędu Miejskiego w Głownie w zamkniętym sejfie.

e) Kopie zapasowe danych finansowych są przechowywane miesiąc, a kopie pozostałych danych dwa tygodnie.

ROZDZIAŁ 9 SPOSÓB, MIEJSCE PRZECHOWYWANIA I POSTĘPOWANIE Z ELEKTRONICZNYMI I PAPIEROWYMI NOŚNIKAMI INFORMACJI ZAWIERAJĄCYMI DANE OSOBOWE

9.1 ELEKTRONICZNE NOŚNIKI INFORMACJI

a) Dane osobowe w postaci elektronicznej - za wyjątkiem kopii bezpieczeństwa - zapisane na: dyskietkach, pamięciach typu flash, dyskach optycznych czy dyskach twardych nie mogą być bez uzasadnienia oraz zgody ADO wynoszone poza siedzibę Urzędu.

b) Każdy użytkownik ma obowiązek zapewnić takie przechowywanie nośników, aby dostęp do nich posiadały osoby wyłącznie upoważnione.

c) Po zakończeniu pracy przez użytkowników, wymienne elektroniczne nośniki informacji są przechowywane w biurku zamykanym na klucz, za które odpowiedzialny jest dany użytkownik.

d) Urządzenia, dyski lub inne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie lub przekazuje wyspecjalizowanej firmie na podstawie umowy w celu zniszczenia. Z czynności zniszczenia ASI sporządza notatkę/protokół z informacją, co i w jaki sposób zostało zniszczone. Notatkę/protokół przechowuje się z dokumentacją, dotyczącą danych osobowych.

e) Urządzenia, dyski lub inne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich ponowne odtworzenie.

f) Urządzenia, dyski lub inne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.

9.2 NOŚNIKI PAPIEROWE

a) Niedopuszczalne jest pozostawianie bez nadzoru i/lub zlecanie wydruków i/lub wykonywania kopii dokumentów zawierających dane osobowe umożliwiając tym samym dostęp do dokumentów osobom nieupoważnionym lub wynoszenie ich poza siedzibę Urzędu i jego lokalizacji.

b) W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu umożliwiającym ich należytą ochronę, w szczególności uniemożliwiającym bezpośredni dostęp osobom nieuprawnionym.

c) W przypadku konieczności udostępniania lub upubliczniania dokumentów, mogą one zostać udostępnione lub upublicznione wyłącznie w części jawnej (udostępnienie danych powszechnie dostępnych lub tych, na udostępnienie których wskazuje przepis prawa).

d) Jeżeli zajdzie potrzeba udostępnienia samej treści dokumentu – należy przed jego udostępnieniem dokonać anonimizacji (poprzez usunięcie danych osobowych).

e) Pracownicy stosują zasadę „czystego biurka", polegającą na nie pozostawianiu zbędnych nośników i dokumentów bez nadzoru.

f) Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie w niszczarce do dokumentów.

ROZDZIAŁ 10 ŚRODKI OCHRONY SYSTEMU PRZED ZŁOŚLIWYM OPROGRAMOWANIEM, W TYM WIRUSAMI KOMPUTEROWYMI

a) Na każdej stacji roboczej jest zainstalowane i aktywne oprogramowanie ochronne/antywirusowe.

b) Każda wiadomość przychodząca i wychodząca „e-mail" jest sprawdzona pod kątem występowania wirusów i oprogramowania szkodliwego - przez oprogramowanie antywirusowe (skanowanie poczty ustawione jako funkcja domyślna oprogramowania AV).

c) Bazy dla oprogramowania antywirusowego aktualizowane są na bieżąco w sposób zautomatyzowany (automatyczne aktualizacje baz wirusów). ASI sprawdza poprawność aktualizacji i baz wirusów na bieżąco.

d) Zabrania się:
   - nieuzgodnionego z ADO/ASI wyłączania mechanizmów ochronnych oraz oprogramowania antywirusowego,
   - pobierania z Internetu plików niewiadomego pochodzenia,
   - odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. (Sprawdzenia dokonuje program skanujący w sposób automatyczny lub gdy nie ma takiej możliwości – dokonywane jest ono ręcznie przez użytkownika),
   - nieuzgodnionej z ASI instalacji lub deinstalacji oprogramowania na stacjach roboczych,
   - w przypadku posiadania takiej możliwości - używania nośników niewiadomego pochodzenia,
   - uruchamiania aplikacji i/lub wczytywania plików z zewnątrz bez ich wcześniejszego sprawdzenia programem antywirusowym, gdy skanowanie nie jest wykonywane automatycznie.

e) ASI przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach.

f) Pracownik użytkujący stację roboczą podłączoną do sieci lokalnej zobowiązany jest udostępnić ją w celu przeprowadzenia przez ASI (lub osobę przez niego wskazaną) weryfikacji prawidłowości realizowanych na nim funkcji ochronnych.

g) Kontrola antywirusowa przeprowadzana jest również na wskazanym komputerze w przypadku zgłoszenia przez użytkownika nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.

h) W przypadku wykrycia wirusów komputerowych i/lub „złośliwego" oprogramowania sprawdzane jest stanowisko komputerowe na którym wirusa wykryto oraz wszystkie wytworzone na tym stanowisku nośniki danych.

ROZDZIAŁ 11 PRZEGLĄDY, KONSERWACJE I NAPRAWY

a) Osobą odpowiedzialną za wykonywanie przeglądów sprzętu i konserwację systemów w Urzędzie jest ASI.

b) Przyjęto zasadę, iż przegląd sprzętu i konserwacja systemów przeprowadzane są na bieżąco według potrzeb określonych przez użytkowników systemu i zgłaszanych przez nich wniosków, kierowanych do Referatu Organizacyjno-Administracyjnego lub bezpośrednio do ASI.

c) Użytkownicy podejmują czynności konserwacji urządzeń takich jak nośniki danych czy wykonują proste czynności konserwacyjne wyznaczone przez ASI po uprzednim ich przeszkoleniu.

d) ASI każdorazowo rozpatruje wniosek użytkownika, badając czy jest on zasadny i w przypadku pozytywnej oceny przystępuje do prac konserwacyjnych lub związanych z przeglądem sprzętu.

e) Przeglądy i konserwacje, wykonywane w siedzibie Urzędu i jej lokalizacjach (np. naprawy, konserwacje) przeprowadzane są zawsze za wiedzą ADO.

f) Przeglądy i konserwacje, wykonywane poza siedzibą Urzędu i jego lokalizacjami (np. naprawy gwarancyjne) przeprowadzane są za wiedzą ADO oraz ASI po sporządzeniu odpowiedniego protokołu (notatki, listu przewozowego, zgłoszenia gwarancyjnego, e-maila).

g) Poddawanie procesowi konserwacji lub przeglądu przez firmę zewnętrzną urządzeń (w tym nośników) zawierających dane osobowe – możliwe jest wyłącznie w siedzibie Urzędu lub jego lokalizacjach chyba, że firma zewnętrzna posiada podpisaną z Urzędem umowę powierzenia danych osobowych i spełnia warunki określone w Ustawie i Rozporządzeniu pozwalające na odpowiednie zabezpieczenie danych osobowych w tym zapewnienie poufności dostępności i integralności danych zawartych na nośnikach, na których wykonywane są czynności serwisowo – konserwacyjne.

h) Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   - **likwidacji** — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
   - **przekazania podmiotowi nieuprawnionemu do przetwarzania danych** — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie lub podpisuje umowę powierzenia zbioru danych osobowych;
   - **naprawy** — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

Burmistrz Głowna
/-/
Grzegorz Janeczek